Differences of subgroups in subgroups [*]

Shkredov I.D.

Annotation.

We prove, in particular, that if $A, \Gamma \subset \mathbb{F}_p^*$, $|\Gamma| < p^{3/4}$ *are two arbitrary multiplicative subgroups satisfying* $A - A \subseteq \Gamma \bigsqcup \{0\}$ *then* $|A| \ll |\Gamma|^{1/3+o(1)}$*. Also, we obtain that for any* $\varepsilon > 0$ *and a sufficiently large subgroup* Γ *with* $|\Gamma| \ll p^{1/2-\varepsilon}$ *there is no representation* Γ *as* $\Gamma = A + B$*, where* A *is another subgroup, and* B *is an arbitrary set,* $|A|, |B| > 1$*. Finally, we study the number of collinear triples containing in a set of* $\mathbb{F}_p$ *and prove a "dual" sum–products estimate.*

1 Introduction

Let p be a prime number and $\mathbb{F}_p$ be the prime filed. For two sets $A, B \subseteq \mathbb{F}_p$ we define its sumset as

$$A + B = \{a + b \ : \ a \in A \,, b \in B\}$$

and similarly its difference set, product set, and so on. A set $S \subseteq \mathbb{F}_p$ is said to be *additively decomposable* if $S = A + B$, $|A|, |B| \geq 2$ and *primitive* otherwise. Sárközy conjectured in [15] that the set of quadratic residues R is primitive and proved that if $R = A + B$, $|A|, |B| \geq 2$ then cardinalities of A, B should be close to $\sqrt{p}$. There are several papers in the direction, see [1], [3], [12], [19], [23], [24]. Sárközy's result was refined slightly in [24], [19] and extended to the case of all multiplicative subgroups by Shparlinski, see [24].

Theorem 1 *Let* $\Gamma \subseteq \mathbb{F}_p$ *be a multiplicative subgroup and for some* $A, B \subseteq \mathbb{F}_p$ *one has*

$$A + B \subseteq \Gamma \,, \tag{1}$$

where $|A|, |B| \geq 2$*. Then*

$$|A|, \, |B| \leq |\Gamma|^{1/2+o(1)} \tag{2}$$

as $|\Gamma| \to \infty$*. In particular, if* $A + B = \Gamma$ *then*

$$|A|, \, |B| = |\Gamma|^{1/2+o(1)} \,.$$

[*] This work was supported by grant Russian Scientific Foundation RSF 14–11–00433.

Note that if it is known that A and B have comparable sizes than one do not need in the restriction $|A|,|B| \ge 2$ to get (2). Also the inclusion (1) can be replaced by a little bit wider one, namely, $A+B \subseteq \Gamma \bigsqcup \{0\}$, see the proof from [24].

In the paper we consider a particular case when A or B is contained in some shift of a multiplicative subgroup. It turns out that the exponent $1/2$ from (2) can be refined in the situation. Let us formulate our result in the simplest symmetric case (that is $B=-A$). Denote by $\mathbb{F}_p^*$ the set $\mathbb{F}_p \setminus \{0\}$.

Theorem 2 *Let $A, \Gamma \subseteq \mathbb{F}_p$ be multiplicative subgroups. Suppose that for some $\xi \in \mathbb{F}_p^*$ one has*

$$A - A \subseteq \xi \Gamma \bigsqcup \{0\} \,. \tag{3}$$

If $|\Gamma| < p^{3/4}$ then

$$|A| \ll |\Gamma|^{1/3+o(1)} \,.$$

If $|\Gamma| \ge p^{3/4}$ then

$$|A| \ll \min \left\{ \frac{|\Gamma| \log^{1/2} p}{\sqrt{p}}, \sqrt{p} \right\} \,.$$

In particular, Theorem 2 implies that for any Γ with $|\Gamma| \ll p^{1-o(1)}$ one has $\Gamma \bigsqcup \{0\} \neq A - A$, where size of Γ is sufficiently large. What can be said in the non–symmetric situation? In [23] the following result on the decompositions was proved.

Proposition 3 *Let $\varepsilon \in (0,1]$ be a real number, $A, \Gamma \subset \mathbb{F}_p^*$ be sufficiently large multiplicative subgroups, and $B \subseteq \mathbb{F}_p$ be an arbitrary nonempty set. If $|\Gamma \cap A| \ll |A|^{1-\varepsilon}$ and $|\Gamma| \ll p^{1-\varepsilon/6}$, then Γ has no nontrivial representations as $\Gamma = A + B$.*

Now we can drop additional assumptions on the intersection A and Γ.

Theorem 4 *Let $\varepsilon \in (0,1]$ be a real number. Let also $A, \Gamma \subset \mathbb{F}_p^*$ be two sufficiently large multiplicative subgroups, $|\Gamma| \le p^{1/2-\varepsilon}$, and $B \subseteq \mathbb{F}_p$ be an arbitrary nonempty set. Then Γ, $\Gamma \bigsqcup \{0\}$ has no nontrivial representations as $\Gamma = A + B$.*

In the proof of Theorem 4 we refine condition (3) and replace it by a more flexible, namely,

$$\xi A + \eta A \subseteq \Gamma \bigsqcup \{0\} \,, \tag{4}$$

where $\xi, \eta \in \mathbb{F}_p^*$ are arbitrary. Moreover, one can consider large subsets of ξA, ηA satisfying inclusion (4) and even take different subgroups A_1, A_2 of comparable sizes, see Theorem 26 and Corollary 28 of section 5. Besides one can deal with the intersections of the form $(\xi A + \eta A) \cap \Gamma$ instead of inclusion (4), see Proposition 35 of section 6.

In [12] the following problem was considered. Let as above $R \subset \mathbb{F}_p^*$ be the subgroup of quadratic residues. Can it be $R \doteq A - A$, that is any $x \in R$ is represented as a difference of two elements of A in a unique way and $A - A \subseteq R \bigsqcup \{0\}$? The authors of [12] proved, in particular, that for any $\xi \in \mathbb{F}_p^*$ one cannot has $R \doteq \xi A - \xi A$, where A is a multiplicative subgroup. In section 6, we obtain a generalization, see Corollary 30 as well as remarks below the corollary.

Theorem 5 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be two multiplicative subgroups. Suppose that $A - A = \xi\Gamma \sqcup \{0\}$ for some $\xi \in \mathbb{F}_p^*$ and $(A \circ A)(x) = c$ is a constant onto Γ. Then $|A|^2 - |A| = c|\Gamma|$ and either $|\Gamma| = O(1)$ or $|\Gamma| \gg \frac{p}{\log p}$.*

Let us say a few words about the methods of the proving of Theorem 1 and similar results and compare them with our new approach. Suppose that for some set S, we have $S = A + B$. The main observation of papers [15], [3], [24], see also [20] is the following. Take an arbitrary positive integer k and any elements $b_1, \dots, b_k \in B$. Then by the definition of sumset, we have

$$A \subseteq (S - b_1) \bigcap (S - b_2) \cdots \bigcap (S - b_k) . \qquad (5)$$

Thus, if S is a sumset then there are large intersections of S with its shifts of form (5). On the other hand, in the case of large multiplicative subgroups one can use analytical tools (see e.g. Lemma 19 below) to show that for $x_1, \dots, x_k \in \mathbb{F}_p$ there is a uniform upper bound

$$|(S + x_1) \bigcap (S + x_2) \cdots \bigcap (S + x_k)| \ll p^{1/2+o(1)} ,$$

provided by $x_1, \dots, x_k$ are nonzero and pairwise distinct elements. For smaller subgroups the analogous result from [25] makes the job.

Theorem 6 *Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup, $k \ge 1$ be a positive integer, and $x_1, \dots, x_k$ be different nonzero elements. Let also*

$$32k2^{20k\log(k+1)} \le |\Gamma| , \quad p \ge 4k|\Gamma|(|\Gamma|^{\frac{1}{2k+1}} + 1) .$$

Then

$$|\Gamma \bigcap (\Gamma + x_1) \bigcap \dots (\Gamma + x_k)| \le 4(k+1)(|\Gamma|^{\frac{1}{2k+1}} + 1)^{k+1} . \qquad (6)$$

The same holds if one replace Γ in (6) by any cosets of Γ.

Thus, theorem above asserts us that $|\Gamma \bigcap (\Gamma + x_1) \bigcap \dots (\Gamma + x_k)| \ll_k |\Gamma|^{\frac{1}{2}+\alpha_k}$, provided by $1 \ll_k |\Gamma| \ll_k p^{1-\beta_k}$, where α_k, β_k are some sequences of positive numbers, and $\alpha_k, \beta_k \to 0$, $k \to \infty$. A little bit better bounds can be found in [23].

So, using inclusion (5), combining with the analytical tools or Theorem 6, we obtain Theorem 1. Now, the main question is: can we prove primitivity of multiplicative subgroups in this way, i.e. just combining upper bounds on intersections of the same strength as in (6) and some random properties of Γ as smallness of its Fourier coefficients, e.g.? As was pointed in [19], [20] the answer is no. To see this consider so–called "random sumsets" example from [20]. Let $A \subseteq \mathbb{F}_p$ be a random set of size $o(\sqrt{p})$, say. The set $A + A$ is what we call a random sumset. It easy to see that $A + A$ has rather random behaviour, excepting nonrandom property (5), of course. Thus, to prove that a set is primitive we cannot use just random properties of the set or upper bounds for the intersections as in (6). We need in different tools. For example, the first author observed in [19] that quadratic residues R is an (almost) perfect difference set, that is the function $f(x) = |\{r_1 - r_2 \ : \ r_1, r_2 \in R\}$ is (almost) constant on $\mathbb{F}_p \setminus \{0\}$. Certainly, random sets have no such a property. This allowed him to prove that R cannot be represented in the form $A + A$ and even to be close to $A + A$ in some sense.

In the article we use another nonrandom property of multiplicative subgroups. Suppose for simplicity that we are in a symmetric situation, that is $A-A \subseteq \Gamma \bigsqcup \{0\}$ and $|A| \sim |\Gamma|^{1/2+o(1)}$. One can assume that $A^* \subseteq \Gamma$, where $A^* = A \backslash \{0\}$ and $1 \in A^*$. Then it is easy to see that $A^*/A^* \subseteq \Gamma \cap (\Gamma+1)$. If $|\Gamma| < p^{3/4}$ then in view of Theorem 6 it gives us $|A^*/A^*| \le |\Gamma \cap (\Gamma+1)| \ll |\Gamma|^{2/3}$ and the bound implies a non–trivial lower bound for the multiplicative energy of A, namely, $\mathsf{E}^\times (A) \ge |A|^{8/3+o(1)}$, see the definition in section 2. Certainly, a random set A has no such a property and hence we have separated from the random sumset case. Unfortunately, the lower bound for the multiplicative energy is not enough to prove our main results because of weakness of estimate (6). In the proof we use a stronger lower bound for average value of common energies $\mathsf{T}(A) := \sum_{a_1,a_2 \in A} \mathsf{E}^\times (A-a_1, A-a_2)$, see section 4. This quantity appears in papers [6], [14], [22] and others. It was showed in [22] that, in contrary, $\mathsf{T}(A)$ is small for any multiplicative subgroup A and we arrive to a contradiction. Thus, in principle, the methods of the paper work for arbitrary sets A with small $\mathsf{T}(A)$. For example, they work when A is an arithmetic progression, for the contrary to the subgroup case (on the other hand, we are crucially need in the fact that the container set Γ is a subgroup). Finally, we have deal with subgroups of small size only to separate from the case of the largest subgroup, namely, $\mathbb{F}_p^*$ which is, clearly, additively decomposable in many ways.

The paper is organized as follows. In section 2 we explain some of notation that will be used later and give auxiliary results on matrices. Section 3 is also devoted to a notation required for the operator technique from [16, 18]. In the next section 4 we prove Theorem 2. The methods here are elementary and do not require eigenvalues approach from [16, 18] as well as the notation from the previous section. Unfortunately, these elementary observations work just in the difference case (3). The general situation is considered in section 5. In particular, here we get Theorem 4. The method of the proving allows us to obtain Theorem 5 in next section 6. In the last section 7 we discuss further properties of the quantity $\mathsf{T}(A)$ and prove, in particular, a "dual" (that is replacing the addition by the multiplication and vice versa) sum–products estimate, concerning the sum $\sum_{c \in C} \mathsf{E}^\times (A-c, B)$, see Proposition 33 below.

The author is grateful to Dmitry Zhelezov, Elena Solodkova for useful discussions and Peter Hegarty as well as Göteborg University and Chalmers University for their hospitality.

2 Notation and auxiliary results

In the paper we use the same letter to denote a set $S \subseteq \mathbb{F}_p$ and its characteristic function $S : \mathbb{F}_p \to \{0,1\}$. By $|S|$ denote the cardinality of S.

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ be two functions. Put

$$(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y) g(x-y) \quad \text{ and } \quad (f \circ g)(x) := \sum_{y \in \mathbb{F}_p} f(y) g(y+x) \qquad (7)$$

If $\gamma \in \mathbb{F}_p^*$ then $f^\gamma (x) := f(\gamma x)$. Put $\mathsf{E}^+(A,B)$ for the *additive energy* of two sets $A, B \subseteq \mathbb{F}_p$ (see e.g. [26]), that is

$$\mathsf{E}^+(A,B) = |\{ a_1 + b_1 = a_2 + b_2 \ : \ a_1, a_2 \in A,\, b_1, b_2 \in B \}| \,.$$

If $A = B$ we simply write $\mathsf{E}^{+}(A)$ instead of $\mathsf{E}^{+}(A, A)$. Clearly,

$$\mathsf{E}^{+}(A,B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x) \,.$$

Note also that

$$\mathsf{E}^{+}(A,B) \le \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\} \,. \tag{8}$$

In the same way define the *multiplicative energy* of two sets $A, B \subseteq \mathbb{F}_p$

$$\mathsf{E}^{\times}(A,B) = |\{a_1 b_1 = a_2 b_2 ~:~ a_1, a_2 \in A,\, b_1, b_2 \in B\}| \,.$$

Certainly, multiplicative energy $\mathsf{E}^{\times}(A,B)$ can be expressed in terms of multiplicative convolutions, similar to (7).

Denote by

$$\mathcal{C}_{k+1}(f_1, \dots, f_{k+1})(x_1, \dots, x_k)$$

the function

$$\mathcal{C}_{k+1}(f_1, \dots, f_{k+1})(x_1, \dots, x_k) = \sum_z f_1(z) f_2(z + x_1) \dots f_{k+1}(z + x_k) \,.$$

Thus, $\mathcal{C}_2(f_1, f_2)(x) = (f_1 \circ f_2)(x)$. If $f_1 = \dots = f_{k+1} = f$ then write $\mathcal{C}_{k+1}(f)(x_1, \dots, x_k)$ for $\mathcal{C}_{k+1}(f_1, \dots, f_{k+1})(x_1, \dots, x_k)$.

We conclude by two auxiliary results. The first one is from the ordinary theory of matrix inequalities, see e.g. [7].

Lemma 7 *Let M be a normal $(n \times n)$–matrix with eigenvalues $\mu_1, \dots, \mu_n$, and let f be an arbitrary convex function of n real variables. Then*

$$\max_{x_1, \dots, x_n} f(\langle M x_1, x_1 \rangle, \dots, \langle M x_n, x_n \rangle) = \max_{i_1, \dots, i_n} f(\mu_{i_1}, \dots, \mu_{i_n}) \,,$$

where the maximum on the left-hand side is taken over all orthonormalized systems of vectors $x_1, \dots, x_n$, and the right-hand maximum over an arbitrary permutation of the numbers $\{1, 2, \dots, n\}$.

The second lemma is also rather standard, see Theorem 2.5.4 of [7].

Lemma 8 *Let $M = (m_{ij})$ be any $(n \times n)$–matrix with eigenvalues $\mu_1, \dots, \mu_n$. Then*

$$\sum_{j=1}^{n} |\mu_j|^2 \le \sum_{i,j=1}^{n} |m_{ij}|^2 \,,$$

and the equality iff M is a normal matrix.

We finish the section by two results from additive combinatorics. The first one is the famous Balog–Szemerédi–Gowers theorem.

Theorem 9 *Let $A, B \subseteq \mathbf{G}$ be two sets such that $\mathsf{E}^+(A,B) \ge |A|^{3/2}|B|^{3/2}/K$. Then there are $x, y \in \mathbf{G}$ and a symmetric set $H \subseteq \mathbf{G}$ with $|A \cap (H+x)|, |B \cap (H+y)| \gg K^{-M}|H|$, further, $|A|, |B| \ll K^M|H|$ and $|H+H| \ll K^M|H|$. Here $M > 0$ is an absolute constant.*

The second result is due to D. Zhelezov [27].

Theorem 10 *Let $A, B, C \subset \mathbb{F}_p$ be three sets, $|A| = |B| = |C| \le \sqrt{p}$. Then for any fixed $d \neq 0$ holds*

$$\max\{|AB|, |(A+d)C|\} \gg |A|^{1+1/26} \,.$$

All logarithms are base 2. Signs $\ll$ and $\gg$ are the usual Vinogradov's symbols. If we have a set A then we will write $a \lesssim b$ or $b \gtrsim a$ if $a = O(b \cdot \log^c |A|)$, $c > 0$.

3 On operators over multiplicative subgroups

Let $\mathbf{G}$ be an abelian group. Let also $g : \mathbf{G} \to \mathbb{C}$ be a function, and $A \subseteq \mathbf{G}$ be a finite set. By T^g_A denote the matrix with indices in the set A

$$\mathrm{T}^g_A(x,y) = g(x-y)A(x)A(y) \,. \tag{9}$$

It is easy to see that T^g_A is hermitian iff $\overline{g(-x)} = g(x)$. The corresponding action of T^g_A is

$$\langle \mathrm{T}^g_A a, b \rangle = \sum_z g(z)(\overline{b} \circ a)(z) \,.$$

for any functions $a, b : A \to \mathbb{C}$. In the case $\overline{g(-x)} = g(x)$ by $\mathrm{Spec}\,(\mathrm{T}^g_A)$ we denote the spectrum of the operator T^g_A

$$\mathrm{Spec}\,(\mathrm{T}^g_A) = \{\mu_1 \ge \mu_2 \ge \dots \ge \mu_{|A|}\} \,.$$

Write $\{f\}_\alpha$, $\alpha \in [|A|]$ for the corresponding eigenfunctions. Let us note two simple formulas

$$\sum_{\alpha=1}^{|A|} \mu_\alpha = g(0)|A| \,, \tag{10}$$

and

$$\sum_{\alpha=1}^{|A|} |\mu_\alpha|^2 = \sum_x |g(x)|^2 (A \circ A)(x) \,. \tag{11}$$

General theory of such operators was developed in [16, 18].

Now we consider the operators of a special form. Let p be a prime number, $q = p^s$ for some integer $s \ge 1$. Let $\mathbb{F}_q$ be the field with q elements, and let $\Gamma \subseteq \mathbb{F}_q$ be a multiplicative subgroup. We will write $\mathbb{F}^*_q$ for $\mathbb{F}_q \setminus \{0\}$. Denote by t the cardinality of Γ, and put $n = (q-1)/t$. Let also $\mathbf{g}$ be a primitive root, then $\Gamma = \{\mathbf{g}^{nl}\}_{l=0,1,\dots,t-1}$. Let $\{\chi_\alpha(x)\}_{\alpha \in [t]}$ be the orthogonal family of multiplicative characters on Γ and $\{f_\alpha(x)\}_{\alpha\in[t]}$ be the correspondent orthonormal family, that is

$$f_\alpha(x) = |\Gamma|^{-1/2}\chi_\alpha(x) = |\Gamma|^{-1/2}\cdot e\left(\frac{\alpha l}{t}\right)\,, \quad x = \mathbf{g}^{nl}\,, \quad 0\le l < t\,. \tag{12}$$

In particular, $f_\alpha(x) = \chi_\alpha(x) = 0$ if $x\notin\Gamma$. Clearly, products of such functions form a basis on Cartesian products of Γ.

If $\varphi : \Gamma\to\mathbb{C}$ be a function then denote by $c_\alpha(\varphi)$ the correspondent coefficients of φ relatively to the family $\{f_\alpha(x)\}_{\alpha\in[t]}$. In other words,

$$c_\alpha(\varphi) := \langle\varphi, f_\alpha\rangle = \sum_{x\in\Gamma}\varphi(x)\overline{f_\alpha(x)}\,, \qquad \alpha\in[|\Gamma|]\,.$$

The method of the paper based on the lemma, which was proved mainly in [16]. We give the proof for the sake of completeness. Further results on the spectrum of operators connected with multiplicative subgroups can be found in [20].

Lemma 11 *Let $\Gamma\subseteq\mathbb{F}_q^*$ be a multiplicative subgroup. Suppose that $H(x,y) : \Gamma\times\Gamma\to\mathbb{C}$ satisfies two conditions*

$$H(y,x) = \overline{H(x,y)} \quad \text{and} \quad H(\gamma x,\gamma y) = H(x,y)\,, \quad \forall\gamma\in\Gamma\,. \tag{13}$$

Then the functions $\{f_\alpha(x)\}_{\alpha\in[|\Gamma|]}$ form the complete orthonormal family of the eigenfunctions of the operator $H(x,y)$.

Proof. The first property of (13) says that H is a hermitian operator, so it has a complete orthonormal family of its eigenfunctions. Consider the equation

$$\mu f(x) = \Gamma(x)\sum_{y\in\Gamma} H(x,y)f(y)\,, \tag{14}$$

where μ is some number and $f : \Gamma\to\mathbb{C}$ is unknown function. It is sufficient to check that any $f = \chi_\alpha$, $\alpha\in[|\Gamma|]$ satisfies the equation above. Indeed, making a substitution $x\to x\gamma$ into (14) and using the characters property, we obtain

$$\mu f(x)f(\gamma) = \Gamma(x\gamma)\sum_y H(\gamma x,y)f(y) = \Gamma(x)\sum_y H(\gamma x,\gamma y)f(\gamma y) = \Gamma(x)f(\gamma)\sum_y H(x,y)f(y)\,,$$

where the second property of (13) has been used. Thus, it remains to check (14) just for one $x\in\Gamma$. Choosing the number μ in an appropriate way we attain the former. This completes the proof. $\Box$

Corollary 12 *Let $\Gamma\subseteq\mathbb{F}_q^*$ be a multiplicative subgroup and g be any Γ–invariant real function. Then the operator T^g_Γ is normal.*

4 First results

In the section we have deal with the quantity $\mathsf{T}(A,B,C,D)$, see [14], [22] (T for collinear *triples*)

$$\mathsf{T}(A,B,C,D) := \sum_{c\in C,\, d\in D} \mathsf{E}^{\times}(A-c, B-d)\,. \tag{15}$$

Clearly, $\mathsf{T}(A,B,C,D)$ enjoy the following invariance property

$$\mathsf{T}(A-x,B-y,C-x,D-y) = \mathsf{T}(A,B,C,D)\,, \qquad \forall x,y \tag{16}$$

as well as

$$\mathsf{T}(\lambda A,\mu B,\lambda C,\mu D) = \mathsf{T}(A,B,C,D)\,, \qquad \forall \lambda,\mu \neq 0\,. \tag{17}$$

If $A=B$, $C=D$ then denote by $\mathsf{T}(A,C)$ the quantity $\mathsf{T}(A,A,C,C)$. If $A=B=C=D$ then we write $\mathsf{T}(A)$ for $\mathsf{T}(A,A,A,A)$. Let us make a few remarks about the quantity $\mathsf{T}(A,B,C,D)$. It is easy to check that

$$\mathsf{T}(A,B,C,D) = \sum_{x,x'\neq 0} \sum_{\lambda} \mathcal{C}_3(C,A,A)(x,\lambda x)\cdot \mathcal{C}_3(D,B,B)(x',\lambda x')+$$

$$+\,\theta(|A\cap C||B|^2|D| + |B\cap D||A|^2|C| + 2|A\cap C||B\cap D||A||B|)\,, \tag{18}$$

where $|\theta|\le 1$. Three error terms in (18) are usually negligible. Denote by $\mathsf{T}^*(A,B,C,D)$ the rest. Thus, in the symmetric case $A=B$, $C=D$ one has

$$\mathsf{T}^*(A,C) = \sum_{\lambda} \left(\sum_{x\neq 0} \mathcal{C}_3(C,A,A)(x,\lambda x) \right)^2\,. \tag{19}$$

Finally, because $\mathsf{E}^{\times}(A-c,B-b) \ge |A||B|$ it follows that $\mathsf{T}(A,B,C,D) \ge |A||B||C||D|$. It turns out that there is the same upper bound for $\mathsf{T}(A)$ (up to logarithmic factors) in the case of cosets of a multiplicative subgroup A. The proof based on the following lemma of Mit'kin [13], see also [10], [23] and [25].

Lemma 13 *Let $p>2$ be a prime number, Γ,Π be subgroups of $\mathbb{F}_p^*$, M_Γ, M_Π be sets of distinct coset representatives of Γ and Π, respectively. For an arbitrary set $\Theta\subset M_\Gamma\times M_\Pi$ such that $(|\Gamma||\Pi|)^2|\Theta| < p^3$ and $|\Theta|\le 33^{-3}|\Gamma||\Pi|$, we have*

$$\sum_{(u,v)\in\Theta} \Big|\{(x,y)\in \Gamma\times\Pi ~:~ ux+vy=1\}\Big| \ll (|\Gamma||\Pi||\Theta|^2)^{1/3}. \tag{20}$$

Using the above lemma, the required upper bound for T was obtained in [22]. It is easy to establish a similar result for larger subgroups A, see Proposition 31 of section 7.

Proposition 14 *Let p be a prime number, Γ,Π be subgroups of $\mathbb{F}_p^*$. Suppose that $|\Gamma||\Pi|<p$. Then for any $\xi\in\mathbb{F}_p^*$, $\eta\in\mathbb{F}_p^*$ one has*

$$\mathsf{T}(\Gamma,\Pi,\xi\Gamma,\eta\Pi) \ll |\Gamma|^2|\Pi|^2\log(\min\{|\Gamma|,|\Pi|\}) + |\Gamma||\Pi|(|\Gamma|^2+|\Pi|^2)\,. \tag{21}$$

It is known that any sets A, B with $A+B \subseteq R$ (R is the set of all quadratic residues) satisfy $|A||B| < p$, see e.g. [1]. Before proving the first main result of the section let us note a very simple estimate for the sizes of A, B with $A+B \subseteq \Gamma \bigsqcup \{0\}$, where Γ is a multiplicative subgroup.

Lemma 15 *Let $\Gamma \subset \mathbb{F}_p^*$ be a multiplicative subgroup, and $A, B \subseteq \mathbb{F}_p$ be two sets. Suppose that $A+B \subseteq \Gamma \bigsqcup \{0\}$. Then $|A||B| < 4p$.*

Proof. Suppose that $|A||B| \ge 4p$. By the assumption $\Gamma \neq \mathbb{F}_p^*$. It follows that $|\Gamma| \le (p-1)/2$. Clearly, we can assume that $|\Gamma|+1 \ge 2\sqrt{p}$. On the other hand by the Cauchy–Davenport theorem [26], we get

$$\frac{p-1}{2} \ge |\Gamma| \ge |A| + |B| - 2 \ge 4\sqrt{p} - 2\,.$$

It follows that $p \ge 59$. We have for any multiplicative subgroup Γ the following upper bound for its Fourier coefficients

$$\max_{\xi \neq 0} |\sum_{x \in \Gamma} e^{2\pi i x \xi / p}| \le \sqrt{p - |\Gamma|}\,,$$

e.g. see [11]. Thus by the conditions $A+B \subseteq \Gamma \bigsqcup \{0\}$, $\Gamma \neq \mathbb{F}_p^*$ and simple Fourier analysis, we get

$$|A||B|p < |A||B|(|\Gamma|+1) + (\sqrt{p-|\Gamma|}+1)(|A||B|)^{1/2}((p-|A|)(p-|B|))^{1/2}\,.$$

After some calculations, we obtain $|A||B| < 4p$ as required. □

Now we can prove the first main result of the section.

Theorem 16 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be two multiplicative subgroups, $|A| < \sqrt{p}$ and $|\Gamma| < p^{3/4}$. Suppose that $A' \subseteq A + s$, $s \in \mathbb{F}_p$ is an arbitrary, and $A' - A' \subseteq \xi\Gamma \sqcup \{0\}$ for some $\xi \in \mathbb{F}_p^*$. Then*

$$|A'|^6 \ll |A|^4 |\Gamma|^{2/3} \log |A|\,.$$

In particular, if $A - A \subseteq \xi\Gamma \sqcup \{0\}$ then $|A| \ll |\Gamma|^{1/3} \log^{1/2} |\Gamma|$.

Proof. In the case $A' = A$ one can assume that $|A| < \sqrt{p}$ for sufficiently large Γ, see Theorem 1. In general case, applying formula (19) with $A = B = C = A'$ and using the Cauchy–Schwarz inequality, we get

$$|A'|^6 \ll (|A'|^3 - 2|A|^2)^2 \le \left(\sum_{x \neq 0,\, \lambda \neq 0} \mathcal{C}_3(A')(x, \lambda x) \right)^2 \ll$$

$$\ll \mathsf{T}(A+s) \cdot |\{\lambda \neq 0 \;:\; \exists x \neq 0 \;\text{ s.t. }\; \mathcal{C}_3(A,A,A)(x,\lambda x) \neq 0\}|\,. \qquad (22)$$

Clearly, if there is $x \neq 0$ with $\mathcal{C}_3(A,A,A)(x,\lambda x) \neq 0$ then $\lambda = (a_1 - a)/(a_2 - a) \neq 0$ for some $a_1, a_2, a \in A$. Since $A - A \subseteq \xi\Gamma \sqcup \{0\}$ it follows that $\lambda \in \Gamma$. But $\lambda - 1 = (a_1 - a_2)/(a_2 - a) \in \Gamma \sqcup \{0\}$. Hence $\lambda \in \Gamma \cap ((\Gamma \sqcup \{0\}) + 1)$. We have $|\Gamma| < p^{3/4}$. By Lemma 13 it follows that

$|\Gamma \cap ((\Gamma \sqcup \{0\}) + 1)| \ll |\Gamma|^{2/3}$. Note, finally, that by (16), we have $\mathsf{T}(A+s) = \mathsf{T}(A)$. Returning to (22) and using Proposition 14, we obtain

$$|A'|^6 \ll |A|^4 \log |A| \cdot |\Gamma|^{2/3}$$

as required. □

Remark 17 *Using a result from [9] on lower bound for the size of the set of the form $C(C+1)$, combining with the arguments of [2], one can prove that for any $B \subset \mathbb{F}_p$, $|B| < \sqrt{p}$, one has $|B \cap (B \pm 1)| \lesssim |BB|^{54/55}$. Thus, the arguments of the proof of Theorem 16 gives a non–trivial upper bound for* **any** *set A with $A - A \subseteq B$, namely, $|A|^6 \lesssim \mathsf{T}(A)|BB/BB|^{54/55}$. Of course, there are another ways to prove the same, applying lower bounds for the cardinality of $(A \pm A)/(A \pm A)$, say. In the case when A is a multiplicative subgroup it is more effectively to use a bound from [22], namely $|\{\frac{a_1 - a}{a_2 - a} \ : \ a, a_1, a_2 \in A\}| \gg \frac{|A|^2}{\log |A|}$, $|A| < \sqrt{p}$. Using the Plünnecke's inequality [26], it gives us $|A| \ll |BB||B|^{-1/2} \log^{1/2} |B|$ and $|A| \lesssim |BB|^{108/55}|B|^{-81/55} \log^{1/2} |B|$.*

Remark 18 *As was pointed in [12] if A, Γ are two multiplicative subgroups and $A - A \subseteq \xi\Gamma \sqcup \{0\}$ then because of $a_1^2 - a_2^2 = (a_1 - a_2)(a_1 + a_2)$ we have $\{a_1 + a_2 \ : \ a_1 \neq a_2,\, a_1, a_2 \in A\} \subseteq \Gamma$. Thus the differences can be reduced to the sumsets, in principle. To make the reverse implication we need in existence of an element $i \in A$ such that $i^2 = -1$. Sumsets and, more generally, sums of two different cosets of subgroups will be considered at the next section.*

To complete the proof of Theorem 2 from the introduction, we need in a rather standard lemma, see e.g. the proof of Lemma 5 from [24]. Let us give a proof for the sake of completeness.

Lemma 19 *Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup, and k be a positive integer. Then for any nonzero distinct elements $x_1, \dots, x_k$ one has*

$$|\Gamma \bigcap (\Gamma + x_1) \bigcap \cdots \bigcap (\Gamma + x_k)| = \frac{|\Gamma|^{k+1}}{(p-1)^k} + \theta k 2^{k+3} \sqrt{p}\,, \tag{23}$$

where $|\theta| \le 1$.

Proof. Let $d = (p-1)/|\Gamma|$. By χ_0 denote the principal character. Then

$$\Gamma(x) = \frac{1}{d} \sum_{\chi \in \mathcal{X}_d} \chi(x) = \frac{1}{d} \left(\chi_0(x) + \sum_{\chi \in \mathcal{X}_d^*} \chi(x) \right)\,,$$

where $\mathcal{X}_d = \{\chi \ : \ \chi^d = \chi_0\}$, $\mathcal{X}_d^* = \mathcal{X}_d \setminus \{\chi_0\}$. Thus, putting $x_0 = 0$, we get

$$|\Gamma \bigcap (\Gamma + x_1) \bigcap \cdots \bigcap (\Gamma + x_k)| = \frac{1}{d^{k+1}} \sum_x \prod_{j=0}^{k} \left(\chi_0(x + x_j) + \sum_{\chi \in \mathcal{X}_d^*} \chi(x + x_j) \right) =$$

$$= \frac{|\Gamma|^{k+1}(p-(k+1))}{(p-1)^{k+1}} + \frac{1}{d^{k+1}} \sum_{l=1}^{k+1} \sum_{\chi_{i_1},\dots,\chi_{i_l} \neq \chi_0} \sum_{x\neq 0} \chi_{i_1}(x+x_{i_1})\dots\chi_{i_l}(x+x_{i_l}) = \frac{|\Gamma|^{k+1}}{(p-1)^k} + \sigma\,.$$

By the well–known Weil's bound in Johnsen's form [8]

$$\left| \sum_{x\neq 0} \chi_{i_1}(x+x_{i_1})\dots\chi_{i_l}(x+x_{i_l}) \right| \le (l+1)\sqrt{p} + 1\,,$$

we get

$$|\sigma| \le \frac{k}{d^{k+1}} + \frac{\sqrt{p}}{d^{k+1}} \sum_{l=1}^{k+1} d^l \binom{k+1}{l} (l+2) \le \sqrt{p} \sum_{l=0}^{k+1} \binom{k+1}{l} (l+2) \le \sqrt{p} k 2^{k+3}$$

as required. □

Lemma above immediately implies a corollary.

Corollary 20 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be two multiplicative subgroups, $|\Gamma| \ge p^{3/4}$. Suppose that $A - A \subseteq \xi\Gamma \sqcup \{0\}$ for some $\xi \in \mathbb{F}_p^*$. Then*

$$|A| \ll \min\left\{ \frac{|\Gamma| \log^{1/2} p}{\sqrt{p}}, \sqrt{p} \right\}\,.$$

Moreover, if a set A' belongs to a shift of the subgroup A, $A' - A' \subseteq \xi\Gamma \sqcup \{0\}$ and $|A| < \sqrt{p}$ then $|A'|^6 \ll |A|^4 \log |A| \cdot |\Gamma|^2 p^{-1}$.

Proof. Using previous lemma in the case $k = 1$, combining with the arguments of the proof of Theorem 16, and taking a half of a set by Lemma 15 if its needed, we obtain $|A| \ll \frac{|\Gamma| \log^{1/2} p}{\sqrt{p}}$. It remains to recall a bound which gives us Lemma 15 for the size of an arbitrary A with $A - A \subseteq \xi\Gamma \sqcup \{0\}$. This completes the proof. □

Corollary above and Theorem 16 give us Theorem 2 from the introduction.

5 The proof of the main result

The next lemma gives us an expression of $\mathsf{T}(A,B,C,D)$ via coefficients c_α of the sets A, B, C, D.

Lemma 21 *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. Let also $A, B, C, D \subseteq \mathbb{F}_p$ be sets, and $A - C, B - D \subseteq \Gamma$. Then*

$$\mathsf{T}(A,B,C,D) = |\Gamma| \sum_{\alpha=1}^{|\Gamma|} \sum_{c\in C} \sum_{d\in D} |c_\alpha(A-c)|^2 |c_\alpha(B-d)|^2\,. \qquad (24)$$

Proof. A direct calculation (or see [20], Lemma 8) shows that

$$\mathsf{E}^{\times}(A,B) = |\Gamma| \sum_{\alpha=1}^{|\Gamma|} |c_\alpha(A)|^2 |c_\alpha(B)|^2$$

for any $A, B \subseteq \Gamma$. Using formula (15) and the fact that $A-c, B-d \subseteq \Gamma$ for any $c \in C$, $d \in D$, we get (24). This completes the proof. $\Box$

Using the eigenvalues technique, we can obtain a rather general result on differences inside multiplicative subgroups.

Proposition 22 *Let $A, \Gamma \subseteq \mathbb{F}_p^*$ be multiplicative subgroups, a set C belongs to a shift of A, $3 \le |C|$, $|A| < \sqrt{p}$. Let also $g : \mathbb{F}_q \to \mathbb{R}^+$ be an arbitrary even Γ–invariant function. Suppose that $C - C \subseteq \xi\Gamma \sqcup \{0\}$ for some $\xi \in \mathbb{F}_p^*$. Then*

$$\left(\sum_x g(x)(C \circ C)(x) \right)^2 \ll \frac{|A|^4 \log |A|}{|C|^2 |\Gamma|} \cdot \sum_x g^2(x) (\Gamma \circ \Gamma)(x) \,. \tag{25}$$

Proof. Without loosing of generality we can assume that $\xi = 1$. Consider the operator T^g_Γ and denote by $\{\mu_\alpha\}_{\alpha=1}^{|\Gamma|}$ its eigenvalues. Note that for any $c \in C$ one has $C - c \subseteq \Gamma \bigsqcup \{0\}$. Putting $C'_c = C \setminus \{c\}$, we have $C'_c - c \subseteq \Gamma$. Thus

$$\sum_x g(x)(C \circ C)(x) - 2(g \circ C)(c) \le \langle \mathrm{T}^g_\Gamma (C'_c - c), C'_c - c \rangle = \sum_\alpha |c_\alpha(C'_c - c)|^2 \mu_\alpha \,.$$

Summing over $c \in C$ and using the condition $|C| \ge 3$, we obtain

$$|C| \sum_x g(x)(C \circ C)(x) \ll \sum_\alpha \mu_\alpha \sum_{c \in C} |c_\alpha (C'_c - c)|^2 \,. \tag{26}$$

Applying the Cauchy–Schwarz inequality, we get

$$|C|^2 \left(\sum_x g(x)(C \circ C)(x) \right)^2 \ll \sum_\alpha |\mu_\alpha|^2 \cdot \sum_\alpha \sum_{c, \tilde{c} \in C} |c_\alpha(C'_c - c)|^2 |c_\alpha (C'_{\tilde{c}} - \tilde{c})|^2 \,.$$

Using formulas (11), (16), Lemma 8, as well as the arguments of the proof of Lemma 21, we get

$$|C|^2 \left(\sum_x g(x)(C \circ C)(x) \right)^2 \ll |\Gamma|^{-1} \sum_x g^2(x)(\Gamma \circ \Gamma)(x) \cdot \sum_{c, \tilde{c} \in C} \mathsf{E}^{\times}(C'_c - c, C'_{\tilde{c}} - \tilde{c}) \le$$

$$\le |\Gamma|^{-1} \sum_x g^2(x)(\Gamma \circ \Gamma)(x) \cdot \sum_{a, \tilde{a} \in A} \mathsf{E}^{\times}(A - a, A - \tilde{a}) = |\Gamma|^{-1} \sum_x g^2(x)(\Gamma \circ \Gamma)(x) \cdot \mathsf{T}(A) \,.$$

Finally, recalling Proposition 14, we obtain (25). This completes the proof. $\Box$

Taking the weight $g(x)$ to be the characteristic function of the set $(-\xi\Gamma) \bigcup \xi\Gamma \bigsqcup \{0\}$, we get Theorem 16 and Corollary 20.

Remark 23 *As we have seen the arguments of the proof of the proposition above allow to replace A onto its a (large) subset $A' \subseteq A$ in spirit of Theorem 16 and Corollary 20 of the previous section. On the other hand there is an asymmetry between A and Γ. We use the group properties of Γ extensively but the only we need about A is that $\mathsf{T}(A)$ is small. For example, if A is an arithmetic progression then our method works similarly.*

Now we can consider the case of general sumsets in multiplicative subgroups. We begin with a lemma which says that the average value of the action of an arbitrary operator T^g_Γ to multiplicative shifts of two functions can be calculated easily. The crucial thing here that the weight g is very general and does not require to be Γ–invariant.

Lemma 24 *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. Let also h_1, h_2 be any functions with supports on Γ and $g : \mathbb{F}_q \to \mathbb{C}$ be an arbitrary function. Then*

$$\frac{1}{|\Gamma|} \sum_{\gamma\in\Gamma} \langle \mathrm{T}^g_\Gamma h^\gamma_1, h^\gamma_2 \rangle = \sum_{\alpha=1}^{|\Gamma|} c_\alpha(h_1) \overline{c_\alpha(h_2)} \cdot \langle \mathrm{T}^g_\Gamma f_\alpha, f_\alpha \rangle \,. \qquad (27)$$

P r o o f. We have $h_1(x) = \sum_\alpha c_\alpha(h_1) f_\alpha(x)$ and $h_2(x) = \sum_\alpha c_\alpha(h_2) f_\alpha(x)$. Thus by the orthogonality of the characters, we have

$$\sum_{\gamma\in\Gamma} \langle \mathrm{T}^g_\Gamma h^\gamma_1, h^\gamma_2 \rangle = \sum_{\gamma\in\Gamma} \sum_{x,y} \mathrm{T}^g_\Gamma(x,y) h_1(\gamma x) \overline{h_2(\gamma x)} =$$

$$= \sum_{\alpha,\beta} c_\alpha(h_1) \overline{c_\beta(h_2)} \cdot \langle \mathrm{T}^g_\Gamma f_\alpha, f_\beta \rangle \cdot \left(\sum_{\gamma\in\Gamma} \chi_\alpha(\gamma) \overline{\chi_\beta(\gamma)} \right) = |\Gamma| \sum_\alpha c_\alpha(h_1) \overline{c_\alpha(h_2)} \cdot \langle \mathrm{T}^g_\Gamma f_\alpha, f_\alpha \rangle \,.$$

as required. □

Using lemma above we prove a general result on sumsets in multiplicative subgroups.

Having a set $Q \subseteq \mathbb{F}_p$ and a multiplicative subgroup Γ denote by $S_\Gamma(Q)$ a minimal Γ–invariant set containing Q. Note that $S_\Gamma(\xi Q) = S_\Gamma(Q)$ for any nonzero ξ. Clearly, $|S_\Gamma(Q)| \le |\Gamma Q| \le |\Gamma||Q|$. Sometimes better estimates holds. For example, if $Q = Q_1 - Q_1$, where $Q_1 \subseteq \Gamma$ then $|S_\Gamma(Q)| \le |\Gamma - \Gamma|$.

Proposition 25 *Let $\Gamma \subset \mathbb{F}_p^*$ be a multiplicative subgroup, $A, B \subseteq \mathbb{F}_p$ be two sets. Let also $g : S_\Gamma(A - A) \to \mathbb{R}^+$ be an arbitrary even Γ–invariant function. Suppose that $A - B \subseteq \Gamma \sqcup \{0\}$ and*

$$|B| \sum_x g(x)(A \circ A)(x) \ge 3 \sum_x g(x)(A \circ B)(x) \,. \qquad (28)$$

Then

$$\left(\sum_x g(x)(A \circ A)(x) \right)^2 \ll \frac{\mathsf{T}(A, B)}{|B|^2 |\Gamma|} \cdot \sum_x g^2(x)(\Gamma \circ \Gamma)(x) \,. \qquad (29)$$

Proof. For any $b \in B$ one has $A - b \subseteq \Gamma \sqcup \{0\}$. Putting $A'_b = A \setminus \{b\}$, we have $A'_b - b \subseteq \Gamma$. Applying Lemma 24 with $h_1 = h_2 = A'_b - b$, we get for any $b \in B$

$$\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\langle \mathrm{T}^g_\Gamma (A'_b - b)^\gamma, (A'_b - b)^\gamma\rangle = \sum_{\alpha=1}^{|\Gamma|} |c_\alpha((A'_b - b)^\gamma)|^2 \cdot \langle \mathrm{T}^g_\Gamma f_\alpha, f_\alpha\rangle \,. \tag{30}$$

Summing over $b \in B$ and using Γ–invariance of g as well as the arguments of the proof of Proposition 22, we see that the left–hand side of (30) is

$$\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{b\in B}\sum_{x,y} g(x-y)(A'_b - b)^\gamma(x)(A'_b - b)^\gamma(y) =$$

$$= \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{b\in B}\sum_{x,y} g(x-y)A'_b(x\gamma + b\gamma)A'_b(y\gamma + b\gamma)\Gamma(x)\Gamma(y) \geq$$

$$\geq \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(|B|\sum_x g(x)(A^\gamma \circ A^\gamma)(x) - 2\sum_{b\in B}\sum_x A(x\gamma + b\gamma)g(x - b\gamma^{-1} + b)\right) \geq$$

$$\geq |B|\sum_x g(x)(A\circ A)(x) - \frac{2}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{b\in B}\sum_x g(x)A(x\gamma + b) \geq$$

$$\geq |B|\sum_x g(x)(A\circ A)(x) - 2\sum_x g(x)(A\circ B)(x) \geq 3^{-1}|B|\sum_x g(x)(A\circ A)(x)\,. \tag{31}$$

Here we have used condition (28). Thus

$$|B|\sum_x g(x)(A\circ A)(x) \ll \sum_\alpha \langle \mathrm{T}^g_\Gamma f_\alpha, f_\alpha\rangle \sum_{b\in B}|c_\alpha((A'_b - b)^\gamma)|^2\,.$$

Applying the Cauchy–Schwarz inequality and Lemmas 7, 8, we obtain

$$|B|^2\left(\sum_x g(x)(A\circ A)(x)\right)^2 \ll \sum_\alpha \langle \mathrm{T}^g_\Gamma f_\alpha, f_\alpha\rangle^2 \cdot \sum_\alpha \sum_{b,\tilde{b}\in B} |c_\alpha((A'_b - b)^\gamma)|^2 |c_\alpha((A'_{\tilde{b}} - \tilde{b})^\gamma)|^2 \leq$$

$$\leq |\Gamma|^{-1}\sum_\alpha |\mu_\alpha(\mathrm{T}^g_\Gamma)|^2 \cdot \sum_{b,\tilde{b}\in B} \mathsf{E}^\times(A-b, A-\tilde{b}) \leq |\Gamma|^{-1}\sum_x g^2(x)(\Gamma\circ\Gamma)(x)\cdot \mathsf{T}(A,B)\,.$$

This concludes the proof. □

Note that the condition on Γ–invariance of g in Proposition 25 is not very important, it needs just for easiest way to obtain estimate (31).

Now we are able to prove the main result of the section.

Theorem 26 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be multiplicative subgroups, $|A| < \sqrt{p}$ and $C, D \subseteq \mathbb{F}_p^*$ be arbitrary sets. Suppose that for some $\xi, \eta \in \mathbb{F}_p^*$ the following holds $C \subseteq \xi A + s$, $D \subseteq \eta A + s$, $s \in \mathbb{F}_p$, $|C| \ge 3$ and*

$$C - D \subseteq \Gamma \bigsqcup \{0\}\,.$$

Then

$$|C|^8 |D|^4 |\Gamma|^2 \ll |A|^8 |S_\Gamma (C - C)| \mathsf{E}^+(\Gamma) \log^2 |A|\,. \tag{32}$$

If $|\Gamma| \ll p^{3/5 - o(1)}$ then $|C|^4 |D|^2 \ll |A|^4 |S_\Gamma(C - C)|^{2/3} \log |A|$.

Proof. Put $S = S_\Gamma(C - C)$. Take $A = C$, $B = D$, $g(x) = S(x)$ and apply Proposition 25. Since $C - C \subseteq S$ and $|C| \ge 3$ it follows that

$$|C|^2 |D| = \sum_x g(x) (C \circ C)(x) \ge 3 |C| |D| \ge \sum_x g(x) (C \circ D)(x)\,.$$

Thus condition (28) of Proposition 25 holds and whence

$$|C|^4 \ll \frac{\mathsf{T}(\xi A + s, \eta A + s)}{|D|^2 |\Gamma|} \sum_x S(x) (\Gamma \circ \Gamma)(x)\,.$$

By the invariance (16) and Proposition 14, we have

$$\mathsf{T}(\xi A + s, \eta A + s) = \mathsf{T}(\xi A, \eta A) \ll |A|^4 \log |A|\,. \tag{33}$$

Further, applying the Cauchy–Schwarz inequality, we get

$$\sigma^2 := \left(\sum_x S(x) (\Gamma \circ \Gamma)(x) \right)^2 \le |S| \sum_x S(x) (\Gamma \circ \Gamma)^2 (x) \le |S| \mathsf{E}^+(\Gamma)\,. \tag{34}$$

Another bound for σ follows from Lemma 13 or see Corollary 6 from [21]

$$\sigma \ll |S|^{2/3} |\Gamma|\,, \tag{35}$$

provided $|\Gamma|^3 |S| \ll p^3$. But

$$|S| \le |C - C| |\Gamma| \le |C|^2 |\Gamma| \ll |\Gamma|^{2 + o(1)}$$

by Theorem 1. Hence, the assumption $|\Gamma| \ll p^{3/5 - o(1)}$ implies $|\Gamma|^3 |S| \ll p^3$. Combining (33) and (34), we get

$$|C|^8 |D|^4 |\Gamma|^2 \ll |A|^8 |S| \mathsf{E}^+(\Gamma) \log^2 |A|\,.$$

Using (33) and (35), we obtain $|C|^4 |D|^2 \ll |A|^4 |S|^{2/3} \log |A|$. This completes the proof. □

Theorem 26 implies an important corollary which beats the exponent $\frac{1}{2}$ of Theorem 1 in a particular case when $A = \xi A$, $B = \eta A$ and A is a subgroup belonging to Γ. We need in a result from [17].

Theorem 27 *Let p be a prime number and $\Gamma \subset \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| < p^{\frac{1}{2}} \log^{-\frac{1}{5}} p$. Then*

$$\mathsf{E}^+(\Gamma) \ll |\Gamma|^{\frac{32}{13}} \log^{\frac{41}{65}} |\Gamma| \,. \qquad (36)$$

Corollary 28 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be multiplicative subgroups, $A \subseteq \Gamma$ and $|\Gamma| < p^{\frac{1}{2}} \log^{-\frac{1}{5}} p$. Suppose that for some $\xi, \eta \in \mathbb{F}_p^*$ the following holds*

$$\xi A + \eta A \subseteq \Gamma \bigsqcup \{0\} \,.$$

Then

$$|A| \ll |\Gamma|^{\frac{19}{39}} \log^{\frac{57}{65}} |\Gamma| \,. \qquad (37)$$

Proof. One can assume that $|A| \geq 3$ because otherwise the result is trivial. Applying formula (32) of Theorem 26 for $C = \xi A$, $D = -\eta A$, combining it with Theorem 27, we get

$$|A|^4 \ll |S| |\Gamma|^{\frac{6}{13}} \log^{\frac{171}{65}} |\Gamma| \,, \qquad (38)$$

where $S = S_\Gamma(\xi(A-A))$. It remains to estimate the size of S. We have $A - A = \bigsqcup_{j=1}^t \xi_j A$, $t = |A-A|/|A| \leq |A|$. By assumption $A \subseteq \Gamma$. It follows that $\Gamma = \bigsqcup_{i=1}^s \eta_i A$, $s = |\Gamma|/|A|$. Whence

$$|S| \leq |\bigcup_{i=1}^s \bigcup_{j=1}^t \eta_i \xi_j A| \leq st|A| \leq |A||\Gamma| \,. \qquad (39)$$

Substituting the last bound into (38), we obtain the required bound for the size of A. This concludes the proof. □

Now we can refine Proposition 3 from the introduction.

Corollary 29 *Let $\varepsilon \in (0,1]$ be a real number. Let also $A, \Gamma \subset \mathbb{F}_p^*$ be two sufficiently large multiplicative subgroups, $|\Gamma| \leq p^{\frac{1}{2}} \log^{-\frac{1}{5}} p$. and $B \subseteq \mathbb{F}_p$ be an arbitrary nonempty set. Then the sets Γ, $\Gamma \bigsqcup \{0\}$ has no nontrivial representations as $\xi A + B$ for any $\xi \in \mathbb{F}_p$.*

Proof. For simplicity assume that $\xi = 1$, otherwise the the proof is similar. We repeat the arguments from [23], so let us miss some details. Consider a multiplicative subgroup $H = \Gamma \cap A$, put $B_\xi = B \cap \xi H$ and denote by k the number of nonempty sets B_ξ. Take $b_j \in B_{\xi_j}$, $j \in [k]$. Thus b_j belong to different cosets relatively to H. Using Lemma 13, the assumption $|\Gamma| < p^{\frac{1}{2}} \log^{-\frac{1}{5}} p$ and the fact that $\Gamma, \Gamma \bigsqcup \{0\} = A + B$ and hence $|A| \ll |\Gamma|^{1/2+o(1)}$, we get

$$k|A| = \sum_{j=1}^k (A \circ \Gamma)(b_j) \ll (|\Gamma||A|k^2)^{1/3} \qquad (40)$$

without any further restrictions on A and Γ. Inequality (40) gives us $k \ll |\Gamma|/|A|^2$. By the pigeonhole principle there is ξ such that $|B_\xi| \ge |B|/k$. We have $H \subseteq A$, and $B_\xi \subseteq B, H$. Hence $H + B_\xi \subseteq \Gamma, \Gamma \bigsqcup \{0\}$. In view of Proposition 3 and our assumption that $A, \Gamma \subset \mathbb{F}_p^*$ are two sufficiently large multiplicative subgroups, we obtain that H is also sufficiently large and $|H| \ge 3$, in particular. Applying formula (32) of Theorem 26 with $A = H$, $C = H$, $D = B_\xi$, $\xi = \eta = 1$, $s = 0$ and using the upper bound for k, we obtain

$$|H|^8 |B|^4 |\Gamma|^2 \ll k^4 |A|^8 |S_\Gamma(H-H)| \mathsf{E}^+(\Gamma) \log^2 |\Gamma| \ll |\Gamma|^4 |S_\Gamma(H-H)| \mathsf{E}^+(\Gamma) \log^2 |\Gamma| \,. \tag{41}$$

By the calculations of Corollary 28, see formula (39), we know that $|S_\Gamma(H-H)| \le |H||\Gamma|$. Because of $k \ll |\Gamma|/|A|^2$ and, trivially, $k \ge |B|/|H|$, we get $|H| \gg |B||A|^2|\Gamma|^{-1}$. Substitution the last estimates into (41) gives us

$$|B|^{11} |A|^{14} \ll |\Gamma|^{10} \mathsf{E}^+(\Gamma) \log^2 |\Gamma| \,.$$

Finally, by Theorem 1, we know that $|A|, |B| \gg |\Gamma|^{1/2 - o(1)}$. Combining the last bound with Theorem 27, we arrive to a contradiction. This completes the proof. $\Box$

Using the full power of the upper bound for the additive energy of a multiplicative subgroup from [20] instead of (36) one can refine the restriction $|\Gamma| \le p^{\frac{1}{2}} \log^{-\frac{1}{5}} p$.

6 On Lev–Sonn's problem

Lev–Sonn's problem on representation of the set of quadratic residues [12] (see also [1]) was discussed in the introduction. In the section we consider a general case of an arbitrary subgroups. First of all let us derive one more consequence of Proposition 22.

Corollary 30 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be two multiplicative subgroups. Suppose that $A - A = \xi\Gamma \sqcup \{0\}$ for some $\xi \in \mathbb{F}_p^*$ and $(A \circ A)(x) = c$ is a constant onto $\xi\Gamma$. Then $|A|^2 - |A| = c|\Gamma|$ and either $|\Gamma| = O(1)$ or $|\Gamma| \gg \frac{p}{\log p}$. If $|\Gamma| \gg \frac{p}{\log p}$ then*

$$\mathsf{E}^+(A) \ll \frac{|\Gamma|}{p} \cdot |A|^2 \log |A| \,, \tag{42}$$

and

$$c^2 \ll \frac{|A|^2 \log |A|}{p} \,. \tag{43}$$

Proof. Because of Γ is nonempty we can assume that $|A| > 1$. The fact that $|A|^2 - |A| = c|\Gamma|$ follows from trivial calculations. By our assumption $(A \circ A)(x)$ is constant onto Γ. In the situation one can choose the weight $g(x)$ in an optimal way, namely, $g(x) = (A \circ A)(x)/(\Gamma \circ \Gamma)(x)$. Clearly, $g(x)$ is an even Γ–invariant nonnegative function. Thus, applying Proposition 22 with $C = A$, we obtain

$$\sum_x \frac{(A \circ A)^2(x)}{(\Gamma \circ \Gamma)(x)} \ll \frac{|A|^2 \log |A|}{|\Gamma|} \,, \tag{44}$$

provided by $|A| < \sqrt{p}$ and $|A| \ge 3$. The last inequality trivially takes place because otherwise $|\Gamma| < |A|^2 \ll 1$. If $|\Gamma| < p^{3/4}$ then by Theorem 1 one can assume that $|A| < \sqrt{p}$ for sufficiently large Γ. Using (44), Lemma 13 and the inequality $|A| > 1$, we get

$$2^{-1}|A|^2 \le |A|^2 - |A| \le \sum_{x\neq 0} (A\circ A)^2(x) \ll |A|^2 \log |A| \cdot |\Gamma|^{-1/3} \,.$$

Because of by Theorem 1, we have $|A| \ll |\Gamma|^{1/2+o(1)}$ (or just use a simple bound $|A| \le |\Gamma|$) it gives us a contradiction for sufficiently large subgroup Γ.

If $|\Gamma| \ge p^{3/4}$ then using Lemma 19 and taking a half of the set A in view of Lemma 15 if its needed, we get by (44) and the previous calculations that

$$3^{-1}\mathsf{E}^+(A) \le \sum_{x\neq 0} (A\circ A)^2(x) \ll \frac{|\Gamma|}{p} \cdot |A|^2 \log |A| \,. \qquad (45)$$

Because of $\mathsf{E}^+(A) \gg |A|^2$ we see from the previous estimate that $|\Gamma| \gg p/\log p$. We have obtained (42) already and to get (42), one can insert the condition $(A\circ A)(x) = c$, $x \in \xi\Gamma$ into (45). This completes the proof. $\Box$

Note that for small Γ it can be $\xi\Gamma \bigsqcup \{0\} = A - A$. For example (see [12]), $p=5$, $A = \{-1,1\}$, $\xi\Gamma = 2\cdot\{-1,1\}$, and $p = 13$, $\Gamma = \{1,3,4,9,10,12\}$, $A = \{2,5,6\} = 2\cdot\{1,3,9\}$. Actually, it is easy to see that for any subgroup A of order $2,3$ one has $\xi\Gamma\bigsqcup\{0\} = A - A$ for some ξ, and $|\Gamma| = |A|^2 - |A|$. Thus, the case $|\Gamma| = O(1)$ is possible in the corollary above.

7 The quantity $\mathsf{T}(A)$ and concluding remarks

In the section we discuss further properties of the quantity $\mathsf{T}(A)$.

First of all, let us prove a simple general upper bound for $\mathsf{T}(A,B,C,D)$, where A,B,C,D are subsets of an arbitrary finite field. Bound (46) below is tight, as the example $q = p^2$ and the case $A = B = C = D$ is a subfield isomorphic to $\mathbb{F}_p$ shows.

Proposition 31 *Let q be a prime power, A be a subgroup of $\mathbb{F}_q^*$. Then for any sets $B,C,D \subseteq \mathbb{F}_q$ one has*

$$\mathsf{T}(A,B,C,D) \le \frac{|A|^2|B|^2|C||D|}{q-1} + |B||C||D|q + \mathsf{T}(A,B,\{0\},D) \,. \qquad (46)$$

Proof. Using formula (15), we get

$$\mathsf{T}(A,B,C,D) = \frac{1}{q-1} \sum_{c\in C} \sum_{d\in D} \sum_{\chi} |(A-c)\check{}(\chi)|^2 |(B-d)\check{}(\chi)|^2 \,,$$

where the summation is taken over all Dirichlet characters χ. The principal character gives us the term $\frac{|A|^2|B|^2|C||D|}{q-1}$. It is well–known, see e.g. [4] that for all non–principal χ, we get

$$|(A-c)\check{}(\chi)|^2 := |\sum_x A(x+c)\overline{\chi(x)}|^2 = |A|^{-2} |\sum_x \sum_{y\in A} A(xy+c)\overline{\chi(x)}|^2 =$$

$$= |A|^{-2} | \sum_{a\in A} \sum_{y \in A} \chi(a-cy)|^2 \le q \,,$$

provided by $c \neq 0$. Using the Parseval's identity, and combining all bounds, we obtain (46). This completes the proof. □

In the case of the prime field one can obtain a simple nontrivial upper bound for the quantity $\mathsf{T}(A)$ which is better than (46) for small sets. The arguments follows [5].

Let us start with an easy combinatorial lemma.

Lemma 32 *Let X be a finite set, $|X| = n$, $A_j \subseteq X$, $j \in [m]$ be a collection of subsets of X, $|A_j| \ge \delta n$, $\delta \in (0,1]$. Suppose that $m \ge 2/\delta$. Then there is a pair (i,j), $i \neq j$ such that $|A_i \cap A_j| \ge 2^{-1} \delta^2 n$.*

Proof. We have

$$\delta m n \le \sigma := \sum_{j=1}^m |A_j| = \sum_{x\in X} \sum_{j=1}^m A_j (x) \,.$$

Using the Cauchy–Schwarz inequality, we get

$$(\delta m n)^2 \le \sigma^2 \le n \sum_{x\in X} \sum_{i,j=1}^m A_i (x) A_j (x) = n \sum_{i,j=1}^m |A_i \cap A_j| = n \left(\sigma + \sum_{i\neq j} |A_i \cap A_j| \right) \,.$$

Applying the assumption $m \ge 2/\delta$, we obtain

$$2^{-1} \delta^2 n^2 m^2 \le 2^{-1} \sigma^2 \le n \sum_{i\neq j} |A_i \cap A_j|$$

as required. □

The next proposition is a "dual" version of the sum–products estimate, where, traditionally, the quantity $\sum_{c\in C} \mathsf{E}^{+} (cA, A)$ is considered, see e.g. [5].

Proposition 33 *Let p be a prime number and $A,B,C \subseteq \mathbb{F}_p$ be three sets, $|A| \le \sqrt{p}$, and $|C| \gg p^\delta$, where $\delta > 0$ be a fixed number. Then there is an absolute constant $\varepsilon = \varepsilon(\delta) > 0$ such that*

$$\sum_{c\in C} \mathsf{E}^{\times} (A-c, B) \ll |A|^{3/2} |B|^{3/2} |C| p^{-\varepsilon} \,. \tag{47}$$

Proof. Put

$$\sum_{c\in C} \mathsf{E}^{\times} (A-c, B) = \frac{|A|^{3/2} |B|^{3/2} |C|}{K} \,, \tag{48}$$

where $K \ge 1$ is some parameter. We need to obtain a lower bound for the number K of the form $K \gg p^\varepsilon$, where $\varepsilon = \varepsilon(\delta) > 0$ is some absolute constant. From formulas (8), (48) it follows that there is a set $C' \subseteq C$, $|C'| \ge |C|/(2K)$ such that for all $c \in C'$ one has $\mathsf{E}^{\times} (A-c, B) \ge$

$|A|^{3/2}|B|^{3/2}/(2K)$. Applying the Balog–Szemerédi–Gowers Theorem 9, we find for any $c \in C'$ a set H_c with $|H_cH_c| \ll K^M|H_c|$, further, $|A|, |B| \ll K^M|H_c|$ and $|(A-c) \cap x_cH_c|, |B \cap y_cH_c| \gg K^{-M}|H_c|$. Here $M > 0$ is an absolute constant. Put $H'_c = A \cap (x_cH_c + c)$, $H''_c = B \cap y_cH_c$ and apply Lemma 32 with $X = A \times B$ and the family of sets $\{H'_c \times H''_c\}_{c \in C'}$. By the lemma and the assumption $|C| \gg p^\delta$, we find $c_1, c_2 \in C'$, $c_1 \neq c_2$ such that the sets $H' = H'_{c_1} \cap H'_{c_2}$, $H'' = H''_{c_1} \cap H''_{c_2}$ have sizes at least $K^{-M_1}|A|$, $K^{-M_1}|B|$, respectively. Here $M_1 > 0$ is another absolute constant. We have

$$(H' - c_1)(H' - c_2) \subseteq x_{c_1}x_{c_2}H_{c_1}H_{c_2}\,. \tag{49}$$

Applying the Plünnecke inequality, see e.g. [26], we obtain

$$K^{-M_1}|B||H_{c_1}H_{c_2}| \ll |H''||H_{c_1}H_{c_2}| \le |H_{c_1}H''||H_{c_2}H''| \le |H_{c_1}H''_{c_1}||H_{c_2}H''_{c_2}| \le$$

$$\le |H_{c_1}H_{c_1}||H_{c_2}H_{c_2}| \ll K^{2M}|H_{c_1}||H_{c_2}| \ll K^{4M}|A||B|\,.$$

Hence $|H_{c_1}H_{c_2}| \ll K^{4M+M_1}|A|$ and thus by inclusion (49), we get

$$|(H' - c_1)(H' - c_2)| \ll K^{4M+M_1}|A| \ll K^{4M+2M_1}|H'|\,. \tag{50}$$

Put $A_* = H' - c_1$, $B_* = H' - c_2$, $C_* = H' - c_1$, $d = c_1 - c_2$. Because of $c_1 \neq c_2$, we see that $d \neq 0$, further, the sets A_*, B_*, C_* have the same size $|H'|$, and by (50) one has $|A_*B_*| \ll K^{4M+2M_1}|H'|$. Further, $|(A_* + d)C_*| = |(H' - c_2)(H' - c_1)|$ and again by (50) the last quantity is bounded as $O(K^{4M+2M_1}|H'|)$. Since $|A| \le \sqrt{p}$, we obtain $|H'| \le \sqrt{p}$. Applying Theorem 10 with $A = A_*$, $B = B_*$, $C = C_*$, we arrive to a contradiction for sufficiently small K. This completes the proof. □

Proposition above has an immediate consequence.

Corollary 34 *Let p be a prime number and $A, B, C, D \subseteq \mathbb{F}_p$ be three sets, $|A| \le \sqrt{p}$, or $|B| \le \sqrt{p}$, and $|C| \gg p^\delta$ or $|D| \gg p^\delta$, where $\delta > 0$ be a fixed number. Then there is an absolute constant $\varepsilon = \varepsilon(\delta) > 0$ such that*

$$\mathsf{T}(A, B, C, D) \ll |A|^{3/2}|B|^{3/2}|C||D|p^{-\varepsilon}\,. \tag{51}$$

Now we obtain an analog of Propositions 22, 25 about the intersections of sumsets and multiplicative subgroups. We thanks to Dmitry Zhelezov who asked us about possible generalizations of our results in this direction.

Proposition 35 *Let $A, \Gamma \subset \mathbb{F}_p^*$ be multiplicative subgroups, $|A| < \sqrt{p}$ and $C, D \subseteq \mathbb{F}_p^*$ be an arbitrary sets. Suppose that for some $\xi, \eta \in \mathbb{F}_p^*$, $s \in \mathbb{F}_p$ the following holds $C \subseteq \xi A + s$, $D \subseteq \eta A + s$ and put $S = S_\Gamma(C - C)$. Then*

$$\left(\sum_{x \in \Gamma} (D \circ C)(x) \right)^8 \ll |D|^4|\Gamma|^{-2}|A|^8|S|\mathsf{E}^+(\Gamma)\log^2|A|\,. \tag{52}$$

If $|\Gamma| \le p^{3/5-o(1)}$ *then*

$$\left(\sum_{x\in\Gamma} (D\circ C)(x) \right)^4 \ll |D|^2 |A|^4 |S|^{2/3} \log |A| \,. \qquad (53)$$

Proof. Put

$$\sigma := \sum_{x\in\Gamma} (D\circ C)(x) = \sum_{x\in D} |\Gamma \cap (C-x)| \,.$$

Take $D' := \{ x\in D ~:~ |\Gamma \cap (C-x)| \ge 2^{-1} \sigma |D|^{-1} \}$. Then

$$\sum_{x\in D'} |\Gamma \cap (C-x)| \ge 2^{-1} \sigma \,. \qquad (54)$$

Applying the Cauchy–Schwarz inequality, we get

$$\sum_{x\in D'} |\Gamma \cap (C-x)|^2 \gg \sigma^2 |D|^{-1} \,. \qquad (55)$$

Returning to (54), we see that for any $x\in D'$ there is a set $C_x \subseteq C$ such that $C_x - x \subseteq \Gamma$. In view of (55) it follows that

$$\sum_{x\in D'} \langle \mathrm{T}^S_\Gamma (C_x - x), C_x - x \rangle = \sum_{x\in D'} |C_x|^2 \gg \sigma^2 |D|^{-1} \,.$$

Using the arguments as in the proofs of Propositions 22, 25, combining with the Cauchy–Schwarz inequality and Lemma 8, we obtain

$$\sigma^4 |D|^{-2} \ll \left(\sum_\alpha \mu_\alpha (\mathrm{T}^S_\Gamma) \sum_{x\in D'} \langle C_x - x, f_\alpha \rangle^2 \right)^2 \ll$$

$$\ll \sum_{x\in S} (\Gamma \circ \Gamma)(x) \cdot \sum_\alpha \sum_{x,x'\in D'} \langle C - x, f_\alpha \rangle^2 \langle C - x', f_\alpha \rangle^2 = |\Gamma|^{-1} \sum_{x\in S} (\Gamma\circ\Gamma)(x) \cdot \mathsf{T}(D,C) \,.$$

By the assumption $C \subseteq \xi A + s$ and $D \subseteq \eta A + s$. Applying Proposition 14, we obtain

$$\sigma^4 \ll |\Gamma|^{-1} |D|^2 |A|^4 \log |A| \cdot \sum_{x\in S} (\Gamma\circ\Gamma)(x) \,.$$

As in the proof of Theorem 26 one can estimate the sum $\sum_{x\in S} (\Gamma\circ\Gamma)(x)$ in two different ways as $(|S| \mathsf{E}^+(\Gamma))^{1/2}$ and $|S|^{2/3}|\Gamma|$, provided $|\Gamma| \le p^{3/5-o(1)}$. This completes the proof. $\Box$

Example 36 *Let* $\xi = 1$, $\eta = 1$, $C = A$, $D = A$, $|A| < \sqrt{p}$, $|\Gamma| \le p^{3/5-o(1)}$. *Let us use a trivial bound for* $\sum_{x\in\Gamma} (A\circ A)(x) \ge |\Gamma \cap (A-A)|$. *Then by (53) one has*

$$|\Gamma \cap (A-A)| \ll |S_\Gamma (A-A)|^{1/6} |A|^{3/2} \log^{1/4} |A| \,.$$

Thus it should be $|S_\Gamma (A-A)| \le |A|^{3-o(1)}$ *to obtain a non–trivial bound for the intersection. The quantity* $|A|^3$ *is some kind of a barrier for usefulness of our bounds.*

The arguments of the proof of Proposition 35 give us a general statement about the connection of $\mathsf{T}(A)$ and the product set/ratio set of popular difference sets.

Proposition 37 *Let* $\mathbf{G}$ *be an abelian group and* $A \subseteq \mathbf{G}$ *be a set. Then*

$$\mathsf{T}(A)|A|^2 \min\{|PP|, |P/P|\} \gg \left(\sum_{x\in P} (A \circ A)(x) \right)^4 . \qquad (56)$$

Finally,

$$\mathsf{T}^*(A) \le |A-A| \sum_x (A \circ A)^3 (x) \,. \qquad (57)$$

Proof. Put $\sigma := \sum_{x\in P} (A\circ A)(x)$. As in the proof of Proposition 35 we find a set $\tilde{A} \subseteq A$ such that for any $a \in \tilde{A}$ there exist $A_a \subseteq A$, $A_a - a \subseteq P$, $|A_a| \ge 2^{-1}\sigma |A|^{-1}$ and

$$\sum_{a\in \tilde{A}} |A_a| \ge 2^{-1} \sigma \,. \qquad (58)$$

For any $a,b \in \tilde{A}$, we have by the Cauchy–Schwarz inequality

$$\mathsf{E}^\times (A-a, A-b) \ge \mathsf{E}^\times (A_a - a, A_b - b) \ge |A_a|^2 |A_b|^2 / \min\{|PP|, |P/P|\} \,.$$

Summing the last bound over all $a, b \in \tilde{A}$, we obtain in view of (58) and the Cauchy–Schwarz inequality

$$\mathsf{T}(A) \min\{|PP|, |P/P|\} \ge \left(\sum_{a\in\tilde{A}} |A_a|^2 \right)^2 \gg \sigma^4 |\tilde{A}|^{-2} \ge \sigma^4 |A|^{-2} \,.$$

To prove (57) just combine (19) and the Cauchy–Schwarz inequality once more time

$$\mathsf{T}^*(A) \le \sum_{x,\lambda} \mathcal{C}^2_3 (A)(x, \lambda x) \cdot |A-A| = \sum_x (A\circ A)^3 (x) \cdot |A-A| \,.$$

This completes the proof. □

References

[1] C. Bachoc, M. Matolcsi and I. Z. Ruzsa, *Squares and difference sets in finite fields,* Integers 13 (2013), paper no. A77, 5 pp.

[2] J. Bourgain, *More on the sum–product phenomenon in prime fields and its applications,* International Journal of Number Theory **1**:1 (2005), 1–32.

[3] C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p,* Monatsh. Math. **169** (2013), 317–328.

[4] P. Erdös, H. N. Shapiro, *On the least primitive roots of a prime,* Pacific J. Math., 7:1 (1957), 861–865.

[5] B. Green, *Sum–product phenomena in $\mathbb{F}_p$: a brief introduction,* 2009, 10 pp., arXiv:0904.2075v1.

[6] T. G. F. Jones, *New quantitative estimates on the incidence geometry and growth of finite sets,* PhD thesis, arXiv:1301.4853 (2013).

[7] R. Horn, C. Johnson, *Matrix Analysis,* Cambridge University Press, Cambridge, 1985, xiii+561 pp.

[8] J. Johnsen, *On the distibution of powers in finite fields,* J. Reine Angew. Math., 251, (1971), 10–19.

[9] T.G.F. Jones, O. Roche–Newton, *Improved bounds on the set $A(A+1)$,* Journal of Combinatorial Theory, Series A 120.3 (2013), 515–526.

[10] S. V. Konyagin, *Estimates for trigonometric sums and for Gaussian sums,* IV International conference "Modern problems of number theory and its applications". Part 3 (2002), 86–114.

[11] S. V. Konyagin, I. Shparlinski, *Character sums with exponential functions,* Cambridge University Press, Cambridge, 1999.

[12] V. F. Lev, J. Sonn, *Quadratic residues and difference sets,* arXiv:1502.06833.

[13] D. A. Mit'kin, *Estimation of the total number of the rational points on a set of curves in a simple finite field,* Chebyshevsky sbornik, **4**:4 (2003), 94–102.

[14] O. Roche–Newton, *A short proof of a near–optimal cardinality estimate for the product of a sum set,* arXiv:1502.05560v1 [math.CO] 19 Feb 2015.

[15] A. Sárközy, *On additive decompositions of the set of the quadratic residues modulo p,* Acta Arith. **155** (2012), 41–51.

[16] T. Schoen, I.D. Shkredov, *Higher moments of convolutions,* J. Number Theory 133 (2013), no. 5, 1693–1737.

[17] I.D. Shkredov, *Some new inequalities in additive combinatorics,* Moscow J. Combin. Number Theory 3 (2013), 237–288.

[18] I.D. Shkredov, *Some new results on higher energies,* Transactions of MMS, 74:1 (2013), 35–73.

[19] I.D. Shkredov, *Sumsets in quadratic residues,* Acta Arith., **164**:3 (2014), 221–244.

[20] I.D. Shkredov, *Energies and structure of additive sets,* Electronic Journal of Combinatorics, 21(3) (2014), #P3.44, 1–53.

[21] I.D. Shkredov, *On exponential sums over multiplicative subgroups of medium size,* Finite Fields and Their Applications **30** (2014), 72–87.

[22] I.D. Shkredov, *On tripling constant of multiplicative subgroups,* arXiv:1504.04522v1.

[23] I. Shkredov, E. Solodkova, I. Vyugin, *Intersections of multiplicative subgroups and Heilbronn's exponential sum,* preprint.

[24] I.E. Shparlinski, *Additive decompositions of subgroups of finite fields,* SIAM J. Discrete Math. **27** (2013), 1870–1879.

[25] I.V. Vyugin, I.D. Shkredov, *On additive shifts of multiplicative subgroups,* Math. Sbornik. 203:**6** (2012), 81–100.

[26] T. Tao and V. Vu, *Additive Combinatorics,* Cambridge University Press (2006).

[27] D. Zhelezov, *On additive shifts of multiplicative almost–subgroups in $\mathbb{F}_p$,* preprint.

I.D. Shkredov
Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991
and
IITP RAS,
Bolshoy Karetny per. 19, Moscow, Russia, 127994
ilya.shkredov@gmail.com